UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

LATERSHIA JONES, individually and on behalf of all others similarly situated, Plaintiff, v. RECEIVABLES PERFORMANCE MANAGEMENT, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Latershia Jones ("Plaintiff") individually and on behalf of all others similarly situated, and by and through her undersigned counsel files this Class Action Complaint against Defendant Receivables Performance Management, LLC ("RPM" or "Defendant") and allege the following based upon personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Defendant provides debt collection services to various businesses, including telecommunications providers, utility providers and financial institutions. To provide these

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

services and in the ordinary course of RPM's business, Defendant acquires, processes, analyzes, and otherwise utilizes the personally identifiable information ("PII") of purported debtors, including, but not limited to, their names and Social Security numbers.

2. By taking possession and control of Plaintiff's and Class members' PII, Defendant assumed a duty to securely store and protect that sensitive information.

3. Defendant breached this duty and betrayed the trust of its clients, Plaintiff and Class members by failing to properly safeguard and protect their PII, thus enabling cybercriminals to steal and misuse it.

4. With this action, Plaintiff and the Class seek to hold Defendant responsible for the harms it caused them resulting from the massive and preventable disclosure of such sensitive and personal information.

5. On or about April 8, 2021, cybercriminals foreseeably accessed files on Defendant's network containing the PII of Plaintiff and millions of other Class Members. Defendant's monitoring practices were so poor that it did not identify this intrusion until May 12, 2021. RPM then reprehensibly waited until November 21, 2022—more than a year later—to begin notifying victims of the Data Breach.

6. Defendant has disclosed that in total, the Data Breach exposed the PII of approximately 3,766,573 people, including names and Social Security numbers.[1]

7. As a result of Defendant's negligent and wrongful conduct, Plaintiff's and Class members' valuable PII was left in the hands of cybercriminals.

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

8. Defendant's misconduct—failing to implement adequate and reasonable data security measures to protect Plaintiff's and Class members' PII, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices and employee training in place to safeguard the PII, failing to honor its promises and representations to protect Plaintiff's and Class members' PII, and failing to provide timely and adequate notice of the Data Breach—caused substantial harm and injuries to Plaintiff and Class members across the United States.

9. Due to Defendant's negligence and data security failures, cybercriminals had access to, and now potentially possess, everything they need to commit identity theft and wreak havoc on the financial and personal lives of millions of individuals.

10. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that Plaintiff's PII has been released to cybercriminals, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and fraudulently using their PII. Plaintiff and Class members have lost time and money responding to and attempting to mitigate the impact of the Data Breach.

11. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages, statutory damages, treble damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorney's fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

THE PARTIES

12. Plaintiff is a citizen and resident of the state of Virginia. Plaintiff received a letter from RPM dated November 21, 2022, notifying her that her PII, including her Social Security number, had been compromised in the Data Breach.

13. Defendant is a Washington limited liability company with its principal place of business at 20818 44th Ave. W., Ste. 240, Lynnwood, WA 98036.

JURISDICTION AND VENUE

14. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendant.

15. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Washington and this District through its headquarters and offices.

16. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

17. For RPM to perform its debt collection services, from which it generates its profits, Defendant collects and stores the PII of individuals, including Plaintiff and the Class.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

18. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to purported debtors, Defendant recognizes the privacy rights of the individuals whose PII Defendant obtains, as evidenced by RPM's publicly available privacy policy ("Privacy Notice").[2] Defendant's Privacy Notice promises to, among other things, maintain the privacy of individuals' PII and not disclose the PII without authorization.

19. Plaintiff and the Class Members reasonably expected that Defendant would implement and maintain reasonable data security measures to protect their PII from foreseeable threats.

20. On or about May 12, 2021, Defendant became aware of a data security incident that impacted its server infrastructure and took Defendant's system offline. Defendant retained a forensic investigation firm that determined Defendant's systems were first accessed by cybercriminals on or about April 8, 2021. During this time, cybercriminals "accessed or acquired" Plaintiff's and Class Members' PII, including Social Security numbers. More than 3,700,000 victims had their PII exposed as a result of the Data Breach.[3]

21. Based on Defendant's acknowledgement that PII was "acquired" by cybercriminals, it is evident that unauthorized cybercriminals did in fact access Defendant's files, and they exfiltrated Plaintiff's and Class members' PII from those files.

22. On information and belief, the PII contained in the files accessed by cybercriminals was not encrypted.

[2] http://www.receivablesperformance.com/PrivacyPolicy.aspx.
[3] https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

23. On information and belief, the cyberattack was targeted at Defendant due to its status as a major debt collector that obtains and stores large amounts of PII.

24. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including the PII of Plaintiff and the Class members.

25. Moreover, while Defendant admits that it learned of the Data Breach in May 2021, Defendant inexplicably waited ***one year and six months*** before Defendant began the process of notifying impacted individuals, such as Plaintiff and Class members.

26. The fact that Defendant needed more than eighteen months after learning of the Data Breach to investigate and begin notifying the impacted individuals of the need for them to protect themselves against fraud and identity theft only highlights the very poor state of Defendant's data security and tracking systems. Defendant was, of course, too late in the discovery, investigation, and notification of the Data Breach.

27. Due to Defendant's inadequate security measures and its delayed notice to victims, Plaintiff and the Class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

28. Defendant had obligations created by industry standards, common law, and its own promises and representations made to Plaintiff and Class members to keep their PII confidential and to protect it from unauthorized access and disclosure.

29. Plaintiff and Class Members had the reasonable expectation that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

31. As a result of Defendant's negligent and wrongful conduct, Plaintiff's and Class members' sensitive PII was left exposed to cybercriminals.

B. Plaintiff's Experience

32. Plaintiff received a letter from RPM dated November 21, 2022, advising her that her information was likely accessed or acquired by cybercriminals in the Data Breach. The letter advised that the PII compromised in the Data Breach included her Social Security number.

33. Because of Defendant's negligence and failure to properly secure the PII in its possession, which negligence and failure led to the Data Breach, Plaintiff's PII has been obtained by cybercriminals.

34. Plaintiff is now under an imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff's life. The imminent risk of identity theft and fraud Plaintiff now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendant in its failure to implement adequate data security protocols, which negligence led to the Data Breach.

35. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, placing credit freezes,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

reviewing accounts statements and other personal information for suspicious activity, and changing passwords and other identifying information.

36. As a direct and proximate result of the Data Breach, Plaintiff will need to have identity theft protection for the foreseeable future.

37. Plaintiff has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff's PII. Additionally, Plaintiff's PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendant and is subject to future wrongful disclosures and/or security breaches so long as Defendant fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

C. Defendant was on Notice of Data Threats in the Industry and of the Inadequacy of its Data Security

38. Defendant was on notice that companies maintaining large amounts of PII are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information.

39. At all relevant times, RPM knew, or should have known, that the PII that it collected was a target for malicious actors. Despite such knowledge, RPM failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that RPM should have anticipated and guarded against.

40. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . Many of them were caused by flaws in . . . systems either online or in stores."[4]

41. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), RPM knew or should have known that its electronic records would be targeted by cybercriminals.

42. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

43. Moreover, PII is a valuable property right.[5] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[6] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[7] It is so valuable to identity

[4] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[5] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[6] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[7] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

44. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

45. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

46. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Cyber Criminals Will Use Plaintiff's and Class Members' PII to Defraud Them

47. Plaintiff's and Class members' PII is of great value to cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

[8] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

48. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[9] For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[10] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

49. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[11]

50. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[12]

51. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and

---

[9] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[10] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[11] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[12] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[13]

52. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

53. For instance, with a stolen Social Security number, which is only one category of the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[15]

54. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[16]

55. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their

---

[13] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.
[14] *Data Breaches Are Frequent*, *supra* note 11.
[15] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[16] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other information for unauthorized activity for years to come.

56. Plaintiff and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

57. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's and Class members' PII.

58. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the kind of PII Defendant made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII, Plaintiff and Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[17]

59. None of this should have happened. The Data Breach was entirely preventable.

E. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' PII

60. Data disclosures and data breaches are preventable.[18] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that

[17] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[18] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[19] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[20]

61. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[21]

62. Defendant obtained and stored Plaintiff's and Class members' PII—including but not limited to, their names Social Security numbers—and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

63. Defendant breached fiduciary duties owed to Plaintiff and the Class as guardian of their PII.

64. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiff's and Class members' PII.

65. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

---

[19] *Id.* at 17.
[20] *Id.* at 28.
[21] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

66. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class members' PII was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

67. The risk of improper disclosure of Plaintiff's and Class members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' PII from that risk left the PII in a dangerous condition.

68. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

69. Plaintiff brings this action under Federal Rule of Civil Procedure 23 against Defendant individually and on behalf of all others similarly situated. Plaintiff asserts all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose personally identifiable information was accessed or acquired as a result of the RPM data breach that is the subject of the notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around November 21, 2022 (the "Nationwide Class" or "Class").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

70. Excluded from the Nationwide Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

71. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

72. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

73. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable.

74. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendant.

75. Adequacy: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class she seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

76. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

77. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;
b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;
c. Whether Defendant's computer systems and data security practices used to protect Plaintiff's and Class members' PII violated the FTC Act, and/or state laws and/or Defendant' other duties discussed herein;
d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach or disclosure;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

j. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class;

and

l. Whether Plaintiff and Class members are entitled to treble damages.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

78. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

79. Defendant gathered and stored the PII of Plaintiff and the Class as part of the operation of its business.

80. Upon accepting and storing the PII of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

81. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff and Class members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

82. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

83. Defendant owed Plaintiff and Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their PII, including taking action to reasonably safeguard

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

84. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

85. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' PII in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

86. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the PII that had been entrusted to it.

87. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

d. Failing to adequately train its employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII;

f. Failing to mitigate the harm caused to Plaintiff and the Class members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their PII.

88. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

89. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

90. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members while it was within Defendant's possession and control.

91. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their PII and mitigate damages.

92. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the PII, and closely reviewing and monitoring bank accounts, credit reports, and financial statements.

93. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

94. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

95. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

SECOND CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

96. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

97. Defendant entered into various written contracts with its clients to perform services that include, but are not limited to, debt recovery services.

98. These contracts were made in part for the benefit of Plaintiff and the Class, as Plaintiff and Class members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Indeed, Defendant knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiff and Class members—would be harmed.

99. Defendant breached the contracts it entered into with its other clients by, among other things, failing to (i) use reasonable data security measures, and (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties.

100. As foreseen, Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

101. Plaintiff and Class members are also entitled to their costs and attorney's fees incurred in this action.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

THIRD CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT (RCW 19.86.010 *ET SEQ.*)
(On Behalf of the Nationwide Class)

102. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

103. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce.

104. Defendant is a "person" as described in RCW 19.86.010(1).

105. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

106. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington.

107. In the course of conducting its business, Defendant committed "unfair acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices ongoing and continue to this date.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

108. Defendant's conduct was also deceptive. Defendant failed to timely notify and concealed from Plaintiff and Class Members the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII.

109. Defendant's above-described "unfair or deceptive acts or practices" affects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

110. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

111. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiff's and Class Members' business and property. Plaintiff and Class members have suffered, and will continue to suffer, actual damages and injury in the form of, *inter alia*, (1) an imminent, immediate, and continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality his or her PII; (5) deprivation of the value of his or her PII, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

112. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

113. Plaintiff, on behalf of Plaintiff and the Class Members, also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of Plaintiff and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained, not to exceed $25,000.00 per class member.

FOURTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

114. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

115. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

116. Defendant owed and owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' PII.

117. Defendant still possesses the PII of Plaintiff and the Class members.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

118. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

119. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

120. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

121. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant provide employee training regarding the dangers and risks inherent in using file-sharing websites;

e. Ordering that Defendant cease transmitting PII via file-sharing websites;

f. Ordering that Defendant cease storing PII on file-sharing websites;

g. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;

h. Ordering that Defendant conduct regular database scanning and security checks; and

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, treble damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: December 2, 2022

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
s/ Kaleigh N. Boyd
Jason T. Dennett, WSBA #30686
Kaleigh N. Boyd, WSBA #52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
kboyd@tousley.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

**pro hac vice applications* forthcoming

Counsel for Plaintiff and the Putative Class